

UNITED STATES DISTRICT COURT

for the
Western District of Washington

In the Matter of the Search of
*(Briefly describe the property to be searched
 or identify the person by name and address)*
 Accounts Associated with 3 Usernames that are
 Stored at Premises Controlled by TextNow, Inc., as
 more fully described in Attachment A

Case No. MJ22-504

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

See Attachment A, which is attached hereto and incorporated herein by this reference.

located in the Northern District of California, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B, which is attached hereto and incorporated herein by this reference.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 U.S.C § 912	Impersonation of an Officer of the United States
18 U.S.C § 1343	Wire Fraud

The application is based on these facts:

- ☒ See Affidavit of Special Agent Matthew Morgan, continued on the attached sheet.

☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.


Pursuant to Fed. R. Crim. P. 4.1, this warrant is presented: ☒ by reliable electronic means; or: ☐ telephonically recorded.


 Applicant's signature

Matthew Morgan, FBI Special Agent
 Printed name and title

- ☐ The foregoing affidavit was sworn to before me and signed in my presence, or
☒ The above-named agent provided a sworn statement attesting to the truth of the foregoing affidavit by telephone.

Date: 10/19/2022


 Judge's signature

City and state: Seattle, Washington

Mary Alice Theiler, United States Magistrate Judge
 Printed name and title

1 The criminals contact the victims by phone and fraudulently inform them that they are in
 2 contempt of court and/or failed to appear in court. The criminals then induce the victims to
 3 send money via digital payment systems, such as Zelle or PayPal, to “resolve” the fabricated
 4 court matters. The conduct under investigation violates multiple provisions of the United
 5 States criminal code, including Title 18 U.S.C. §§ 912 (Impersonation of an Officer of the
 6 United States) and 1343 (Wire Fraud).

7 5. I make this affidavit in support of an application for to search information
 8 associated with the TextNow accounts associated with the following usernames:

- 9 • **usdistricourt.org (TARGET ACCOUNTS 1);**
- 10 • **usdistrictclerkofcou (TARGET ACCOUNTS 2); and**
- 11 • **unitedstatesclerkofc (TARGET ACCOUNTS 3);**

12 collectively, **TARGET ACCOUNTS**, that are stored at premises controlled by TextNow
 13 Inc. (TextNow) and more fully described in Attachment A.

14 6. TextNow is an electronic communications service accepting process at Attn:
 15 Registered Agent of Process for TextNow Inc., GKL Corporate/Search, Inc., Capitol Mall,
 16 Suite 660, Sacramento, CA 95814. TextNow Inc. is the United States-based location for
 17 TextNow, Inc. at 420 Wes Graham Way, 2nd Floor, Waterloo, Ontario, Zip Code N2L 0J6,
 18 Canada.

19 7. The requested warrant would require Text Now to disclose to law enforcement
 20 the material listed on Attachment B.I and would authorize law enforcement officers to search
 21 for and seize the material listed on Attachment B.II.

22 8. As discussed herein, my investigation has developed evidence that the user(s)
 23 of **TARGET ACCOUNTS** has obtained and attempted to obtain fraudulent transfer of funds
 24 by impersonating federal officials. The requested materials are expected to contain further
 25 evidence of fraud and impersonation, as well as evidence that will help the government
 26 further establish and prove the identity of the person(s) who engaged in these fraudulent
 27 activities. Therefore, probable cause exists to believe that the **TARGET ACCOUNTS** will
 28 contain evidence and instrumentalities of the offenses referenced above.

1 9. The facts set forth in this Affidavit are based on my own personal knowledge;
 2 knowledge obtained from other individuals during my participation in this investigation,
 3 including other law enforcement officers; interviews of cooperating witnesses; review of
 4 documents and records related to this investigation; communications with others who have
 5 personal knowledge of the events and circumstances described herein; and information
 6 gained through my training and experience.

7 10. Because this Affidavit is submitted for the limited purpose of establishing
 8 probable cause in support of the application for a search warrant, it does not set forth each
 9 and every fact that I or others have learned during the course of this investigation. I have set
 10 forth only the facts that I believe are necessary to establish probable cause to issue the
 11 requested search warrant.

12 11. This Court has jurisdiction to issue the requested warrant because it is “a court
 13 of competent jurisdiction” as defined by 18 U.S.C. § 2711. Specifically, the Court is “a
 14 district court of the United States . . . that has jurisdiction over the offense being
 15 investigated.” 18 U.S.C. § 2711(3)(A)(i).

16 12. This Affidavit is to be presented electronically pursuant to Local Criminal Rule
 17 CrR 41(d)(3).

18 **STATEMENT OF PROBABLE CAUSE**

19 **A. Investigation Overview**

20 13. In late 2021, federal investigators began receiving a significant volume of
 21 reports of a common fraud scheme in which health care workers were receiving phone calls
 22 from individuals claiming to be U.S. Marshals or other federal officials. The individual
 23 would then inform the health care worker that they had failed to appear in court and could
 24 “resolve” the matter by making a payment to a digital payment system account using
 25 platforms such as Zelle, PayPal, or Google Pay.

26 14. In a specific instance, on March 3, 2022, K.C., a pediatric health care provider
 27 at the Seattle Cancer Care Alliance and Seattle Children’s Hospital, emailed federal
 28 investigators an audio file of a voicemail from an individual who identified himself as United

1 States Marshal Gary Hartnett. The voicemail stated that the individual had “important legal
2 documents” to discuss with K.C. and requested that K.C. return his call at 206-350-9946.

3 15. When K.C. returned the call, the individual stated that the call was being
4 conducted on a recorded line. The individual stated that she had failed to appear as an expert
5 witness in a juvenile case on Monday, February 21, 2022, and now had two warrants out for
6 her arrest. She was further informed by the individual that the United States Marshals had a
7 signed subpoena with her signature obtained by two uniformed officers on Wednesday,
8 January 19, 2022, at 2:07 P.M. The individual asserted that the subpoena had been delivered
9 to her at 825 Eastlake Avenue in Seattle, which is the address for the Seattle Cancer Care
10 Alliance clinic. To resolve this matter, she was instructed by the individual to proceed with
11 either the “criminal process” or “civil process.” For the “criminal process,” she could turn
12 herself in that day and be “apprehended” for up to 72 hours while bond and court dates are
13 reset, and this would be a part of her public record moving forward. Or, to proceed with
14 “civil process,” she would need to secure a civil surety bond with the court and appear at
15 court at 700 Stewart Street in Seattle on the same day to take a signature verification test to
16 prove that it was not her signature on the subpoena. Upon verification, the surety bond
17 payment would be refunded to her.

18 16. The individual provided the following warrant and bond information:
19 Contempt of Court (COC): 7-21-068 with bond of \$1,000 and Failure to Appear (FTA): 46-
20 64-025 with bond of \$1,000. The individual stated he needed to place K.C. on a hold so
21 discuss her payment options with the “clerical clerk Sandra.” He returned to the call and
22 informed K.C. that she could make the \$2000 payment via digital payment systems Zelle or
23 Google Pay to usdistrictcourt.org@gmail.com, the email address associated with **TARGET**
24 **ACCOUNTS 1**. Digital payment systems like Zelle and Google Pay allow users to send
25 money to an account identified by an email address or a phone number.

26 17. K.C. stated that she questioned the validity of the individual’s statements
27 throughout the call. For example, she informed the individual that she could not have signed
28 the subpoena allegedly delivered to the clinic in January because she was not seeing patients

1 at the clinic in January. The individual responded that a secretary or security guard could
2 have signed for her and she was still legally responsible.

3 18. Additionally, although K.C. had returned the call at the number provided in the
4 voicemail (ending in -9946), the phone number that appeared on her caller ID screen was
5 206-370-8600. The individual instructed her to search the internet for the phone number, the
6 search engine associated the phone number with "US Marshals Service" in Seattle.

7 19. The individual insisted that he was a real United States Marshal, and she was
8 indeed in contempt of court for a juvenile case. He further said that there was a no-contact
9 order and gag-order placed by the judge, so if she tried to contact a lawyer or discussed this
10 matter with anyone else, she would forfeit the civil process and be prosecuted under the
11 criminal process that he had previously explained which would ultimately result in her arrest.
12 He also refused to provide any information about the case as it "involved a minor."

13 20. While the individual had K.C. "on hold," she called the United States District
14 Court in Seattle and spoke with court personnel who confirmed that the call was a scam.

15 **B. Google Fraud Accounts**

16 21. On March 31, 2022, this Court authorized a search warrant to search Google
17 account usdisitretcourt.org@gmail.com (Fraud Account 1). In response to that search
18 warrant, Google provided subscriber information that was consistent with the information
19 K.C. provided. The account was created on March 3, 2022, one day before K.C. received the
20 imposter call, and the name associated with the account is "Sandra Kiele," which is
21 consistent with the imposter caller's reference to his "clerical clerk Sandra."

22 22. The contents of the Fraud Account 1 inbox included emails from PayPal,
23 indicating that the account was associated with a PayPal account. Among the
24 communications the account received from PayPal is a message on March 14, 2022, with the
25 subject, "You can no longer do business with PayPal." The message stated that PayPal
26 decided to permanently limit the account due to potential risk associated with it.

27 23. The contents of the Fraud Account 1 inbox also included emails from Venmo,
28 indicating that the account was used to open a Venmo account on or about March 10, 2022.

1 A day later, Fraud Account 1 received a conformation email about a payment of \$380 to the
2 Venmo account from “Brent Lacey” with a memo note of “Restitution fee.” Open source
3 research indicates that a gastroenterologist in Texas is named Brent Lacey.

4 24. The contents of the Fraud Account 1 inbox also included an email from
5 TextNow indicating that the account was associated with a TextNow account.

6 25. In response to the search warrant for Fraud Account 1, Google also provided
7 records showing the other Google accounts that are linked by cookies, signifying that the
8 accounts were accessed by the same device. Among the accounts linked by cookies are
9 usdistrictclerkofcourt.org@gmail.com (Fraud Account 2) and
10 unitedstatesclerkofcourt.org@gmail.com (Fraud Account 3).

11 26. On July 12, 2022, this Court issued an order pursuant to 18 U.S.C. § 2703(d),
12 directing Google to disclose non-content information about ten accounts linked to Fraud
13 Account 1 by cookies, including Fraud Accounts 2 and 3. The subscriber information for the
14 accounts show that Fraud Account 2 was created on March 12, 2022, and Fraud Account 3
15 was created on March 21, 2022.

16 27. According to Google’s records, on multiple days, Fraud Accounts 1, 2, and 3
17 logged into their accounts using the same IP address, suggesting a common user for the
18 accounts. For example, on March 21, 2022, at the exact same time, 22:09:12, all three
19 accounts logged in using IP address 2600:1005:b144:92a4:0:4f:24a5:2c01. Again, on March
20 31, 2022, at the exact same time, 01:35:19, all three accounts logged in using IP address
21 2600:1005:b149:a1a7:0:44:eb85:7a01. Fraud Accounts 1 and 2 used the same IP addresses
22 on four additional dates during March 2022. Fraud Accounts 1 and 3 used the same IP
23 address on one additional date during March 2022.

24 28. In response to the 2703(d) order, Google also provided non-content
25 information about the emails in Fraud Accounts 2 and 3. Both accounts received emails
26 from TextNow. Fraud Account 3 also received 24 emails form PayPal.

C. Zelle and PayPal Fraud Accounts

29. Based on the information K.C. provided and the records Google produced, using Grand Jury subpoenas, investigators sought records associated with Fraud Accounts 1, 2, and 3 from digital payment systems Zelle and PayPal.

30. Zelle's records show a Zelle account associated with Fraud Account 1 received 11 payments between March 8, 2022, and March 28, 2022, for amounts ranging from \$500 to \$3,000. The total amount paid to the account was \$16,200, not including an additional \$3,000 payment that filed to be completed. Although Zelle allows payers to make payments using either a phone number or email address, all 11 payments directed their payments to the Fraud Account 1 email address.

31. Based on open source research conducted on <https://www.hipaaspace.com/>, which publishes healthcare provider data, all 11 payment senders are associated with individuals who are health care workers. For instance, a sender named "Kathryn E. Bakkum," who sent \$3,000 to the Zelle account on March 9, 2022, matches the name of a pediatrician in Akron, Ohio, named Kathryn Elizabeth Bakkum. I interviewed Kathryn Bakkum of Akron, Ohio and she confirmed she sent the \$3,000 payment to a Zelle account associated with Fraud Account 1. She also made two \$1,000 payments to a Venmo user, @AccurateDistrict Court. She made these payments because she received a phone call in which two individuals impersonated law enforcement officials. The callers stated she had multiple warrants for her arrest connected to her failure to appear at court and contempt of court.

32. Another Zelle payment sender named "Jolie Ramesar," who made two payments on March 14, 2022 totaling \$3,500, matches the name of an internal medicine physician who previously worked in Fresno, California. Additionally, several of the payments include payment memos where the senders included notations such as "FTA," "FTA-COC," "Federal side," "COC 221-CV-1113," and "coc34-37-41." These notations are consistent with the contempt of court and failure to appear designations the imposter caller provided K.C as well as multiple other victims.

33. PayPal's records associate Fraud Account 1 with three PayPal accounts, ending in -3018, -5799, and -5482. Fraud Account 2 is associated with one PayPal account, ending in -6793. Fraud Accounts 1 and 3 are both associated with another PayPal account, ending in -3084. Of these five accounts, three accounts (ending in -3018, -3084, and -6793) received payments between March 2022 and May 2022 from sender names that also appear to be health care workers. For instance, for the account ending in -6793 and associated with Fraud Account 2, the sender name for two \$1,000 payments on March 14, 2022 is "Alison Faulkingham MD," which matches the identity of a pediatrician in Bangor, Maine. In another instance, for the account ending in -3084 and associated with Fraud Accounts 1 and 3, the sender name for a \$1,000 payment on March 23, 2022 is "Whole Health Counseling LLC," which matches the name of the practice for a licensed professional counselor in Alexandria, Virginia. The sender's email address is "angela@wholehealthcounselingllc.com," which matches the name of the counselor at the practice.

34. PayPal also provided logs of IP addresses used to access the PayPal accounts associated with Fraud Accounts 1, 2, and 3. A comparison with the IP addresses provided by Google for the three accounts shows logins regularly occur in Eastern Georgia and Alabama.

D. Bo NNANWUBAS

35. The Zelle records and bank records from SunTrust Bank show that the recipient of the funds sent to the Zelle account associated with Fraud Account 1 is Bo NNANWUBAS in Marietta, Georgia. However, open source research shows that NNANWUBAS is currently, and at all times relevant to this investigation, an inmate at Calhoun State Prison in Morgan, Georgia. Federal investigators learned that contraband electronic devices, including cell phones, are ubiquitous at Calhoun State Prison, and the telemarketing scheme identical or similar to the one described above by K.C. is commonly executed by Calhoun State Prison inmates.

36. Using open source research, investigators were able to identify the identities of NNANWUBAS' wife, sister, and mother. Google, Zelle, PayPal, and bank records confirm

1 that the accounts associated with Fraud Accounts 1, 2, and 3, are linked to NNANWUBAS
2 and his family.

3 37. For instance, the subscriber address for three PayPal accounts that received
4 payments from health care workers is an address on Bond Road in Marietta, Georgia. Open
5 source research associates this same address with NNANWUBAS' wife, and it also appears
6 on NNANWUBAS' SunTrust Bank statements. The billing addresses linked to the Google
7 Pay account associated with Fraud Account 1 are also the same Marietta, Georgia address on
8 Bond Road and an address on Early Parkway Drive in Smyrna, Georgia, which investigators
9 have associated with NNANWUBAS' mother and sister.

10 38. Additionally, NNANWUBAS' wife, mother, and sister all receive transfers
11 from the Zelle and PayPal accounts associated with Fraud Accounts 1, 2, and 3. For
12 example, on March 3, 13, and 24, 2022, NNANWUBAS' Zelle account associated with
13 Fraud Account 1 transfers \$500, \$50, and \$450 to his mother's Wells Fargo account. In
14 another instance, on March 14, 2022, within 30 minutes of receiving two \$1,000 payments
15 from Dr. Alison Faulkingham, the PayPal account ending in -6793 and associated with Fraud
16 Account 2, transfers \$2,0000 to NNANWUBAS' sister.

17 **E. TARGET ACCOUNTS**

18 39. In response to a Grand Jury subpoena, TextNow provided subscriber records
19 for **TARGET ACCOUNTS**, which were all registered in March 2022. **TARGET**
20 **ACCOUNTS 1** consists of five phone numbers associated with Fraud Account 1.
21 **TARGET ACCOUNTS 2** consists of three phone numbers associated with Fraud Account
22 2. **TARGET ACCOUNTS 3** consists of five phone numbers associated with Fraud
23 Account 3. For each TextNow account, the subscriber name matches the subscriber name
24 used for its associated Google Account. For instance, the subscriber name for **TARGET**
25 **ACCOUNTS 1** is Sandra Kiele, the same subscriber name for Fraud Account 1.

26 40. TextNow records show **TARGET ACCOUNTS 3** had three separate
27 telephone calls with 850-760-7457 on March 28, 2022. The number 850-760-7457 belongs
28 to Deborah Rigsby. Rigsby was later interviewed and confirmed she had been contacted by

1 two individuals impersonating law enforcement officers. Rigsby eventually sent \$700 to the
2 Zelle account associated with Fraud Account 1. Grand Jury returns from Zelle confirm that a
3 Deborah Rigsby sent \$700 to Fraud Account 1 on March 28, 2022.

4 41. TextNow records also indicate there are currently 584 undeleted text messages
5 associated with **TARGET ACCOUNTS**. Messages were exchanged with 310 unique
6 numbers and **TARGET ACCOUNTS**. Based on my training and experience given the large
7 quantity of unique numbers which communicated with **TARGET ACCOUNTS**, it is likely
8 that there exists evidence of crimes within the undeleted text messages.

9 **BACKGROUND REGARDING PROVIDER'S SERVICES**

10 42. As explained herein, information stored in connection with an online account
11 may provide crucial evidence of the “who, what, why, when, where, and how” of the
12 criminal conduct under investigation, thus enabling the United States to establish and prove
13 each element or alternatively, to exclude the innocent from further suspicion.

14 43. In my training and experience, the information stored in connection with an
15 online account can indicate who has used or controlled the account. This “user attribution”
16 evidence is analogous to the search for “indicia of occupancy” while executing a search
17 warrant at a residence. For example, text communications, contacts lists, and images sent
18 (and the data associated with the foregoing, such as date and time) may indicate who used or
19 controlled the account at a relevant time.

20 44. Further, information maintained by the provider can show how and when the
21 account was accessed or used. For example, as described below, providers typically log the
22 Internet Protocol (IP) addresses from which users access the account, along with the time
23 and date of that access. By determining the physical location associated with the logged IP
24 addresses, investigators can understand the chronological and geographic context of the
25 email account access and use relating to the crime under investigation. This geographic and
26 timeline information may tend to either inculcate or exculpate the account owner.
27 Additionally, information stored at the user’s account may further indicate the geographic
28

1 location of the account user at a particular time (e.g., location information integrated into an
2 image or video sent via text message).

3 45. Stored electronic data may provide relevant insight into the account owner's
4 state of mind as it relates to the offense under investigation. For example, information in the
5 account may indicate the owner's motive and intent to commit a crime (e.g., communications
6 relating to the crime), or consciousness of guilt (e.g., deleting communications in an effort to
7 conceal them from law enforcement).

8 46. In my training and experience, I have learned that TextNow provides a variety
9 of online services, including online calling and messaging services, to the general public.
10 TextNow allows subscribers to obtain Voice Over Internet Protocol ("VoIP") numbers, like

11 **TARGET ACCOUNTS.**

12 47. Subscribers obtain an account by registering with TextNow. When doing so,
13 TextNow asks the subscriber to provide certain personal identifying information. This
14 information includes the subscriber's full name, email address, and preferred username. In
15 my training and experience, such information may constitute evidence of the crimes under
16 investigation because the information can be used to identify the account's user or users, and
17 to help establish who has dominion and control over the account.

18 48. TextNow retains certain transactional information about the creation and use of
19 each account on their systems. This information includes the date on which the account was
20 created, the length of service, records of log-in (i.e., session) times and durations, the types
21 of service utilized, the status of the account (including whether the account is inactive or
22 closed), and other log files that reflect usage of the account. In addition, TextNow has
23 records of the Internet Protocol address ("IP address") used to register the account and the IP
24 addresses associated with particular logins to the account. Because every device that
25 connects to the Internet must use an IP address, IP address information can help to identify
26 which computers or other devices were used to access the account, which can help establish
27 the individual or individuals who had dominion and control over the account
28

49. In general, a text message that is sent to a TextNow subscriber is stored in the subscriber's account on TextNow's servers until the subscriber deletes the message. If the subscriber does not delete the message, the message can remain on TextNow's servers for approximately two years. Similarly, when the subscriber sends a text message, it is initiated at the user's computer, transferred via the Internet to TextNow's servers, and then transmitted to its end destination. TextNow often maintains a copy of the text message sent. Unless the sender of the text message specifically deletes the text message from the TextNow server, the text message can remain on the system for approximately two years.

50. According to its law enforcement guide, TextNow also retains the content of voicemails and media files sent or received by TextNow users. Media files are retained indefinitely for TextNow's paid users but are only retained for approximately 30 days for TextNow's free users. It appears that the **TARGET ACCOUNTS** are free accounts.

51. On July 21, 2022, TextNow confirmed the government's request to preserve the contents of the **TARGET ACCOUNTS** for 90 days.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

52. Pursuant to Title 18, United States Code, Section 2703(g), this application and affidavit for a search warrant seeks authorization to permit TextNow, and their agents and employees, to assist agents in the execution of this warrant. Once issued, the search warrant will be presented to TextNow with direction that it identify the TextNow account described in Attachment A to this affidavit, as well as other subscriber and log records associated with the accounts, as set forth in Section I of Attachment B to this affidavit.

53. The search warrant will direct TextNow to create an exact copy of the specified account and records.

54. I, and/or other law enforcement personnel will thereafter review the copy of the electronically stored data, and identify from among that content those items that come within the items identified in Section II to Attachment B for seizure.

55. Analyzing the data contained in the forensic image may require special technical skills, equipment, and software. It could also be very time-consuming. Searching

by keywords, for example, can yield thousands of “hits,” each of which must then be reviewed in context by the examiner to determine whether the data is within the scope of the warrant. Merely finding a relevant “hit” does not end the review process. Keywords used originally need to be modified continuously, based on interim results. Certain file formats, moreover, do not lend themselves to keyword searches, as keywords, search text, and many common e-mail, database and spreadsheet applications do not store data as searchable text. The data may be saved, instead, in proprietary non-text format. And, as the volume of storage allotted by service providers increases, the time it takes to properly analyze recovered data increases, as well. Consistent with the foregoing, searching the recovered data for the information subject to seizure pursuant to this warrant may require a range of data analysis techniques and may take weeks or even months. All forensic analysis of the data will employ only those search protocols and methodologies reasonably designed to identify and seize the items identified in Section II of Attachment B to the warrant.


56. Based on my experience and training, and the experience and training of other agents with whom I have communicated, it is necessary to review and seize a variety of text communications, chat logs and documents, that identify any users of the subject account and text message sent or received in temporal proximity to incriminating text messages that provide context to the incriminating communications.

CONCLUSION


57. Based on the forgoing, I believe there is probable cause to believe that evidence, instrumentalities, contraband, and/or fruits of violations of Title 18 U.S.C. §§ 912 (Impersonation of an Officer of the United States) and 1343 (Wire Fraud) will be found in the **TARGET ACCOUNTS**, as more fully described in Attachment A to this Affidavit. I therefore request that the Court issue the proposed search warrant authorizing search of the **TARGET ACCOUNTS** and seizure of the items described in Attachment B to this Affidavit.

58. Pursuant to 18 U.S.C. § 2703(g), the government will execute this warrant by serving the warrant on TextNow. Because the warrant will be served on TextNow, who will

1 then compile the requested records and data, reasonable cause exists to permit the execution
2 of the requested warrant at any time in the day or night.

3
4
5 
6 Matthew Morgan, Affiant
7 Special Agent
8 Federal Bureau of Investigation

9 The above-named agent provided a sworn statement attesting to the truth of the
10 contents of the foregoing affidavit on 19th day of October, 2022.

11
12 
13 MARY ALICE THEILER
14 United States Magistrate Judge
15
16
17
18
19
20
21
22
23
24
25
26
27
28

ATTACHMENT A
ACCOUNTS TO BE SEARCHED

The electronically stored data, information and communications contained in, related to, and associated with, including all preserved data associated with the TextNow, Inc. accounts using the following usernames:

- **usdistricourt.org (“TARGET ACCOUNTS 1”);**
- **usdistrictclerkofcou (“TARGET ACCOUNTS 2”); and**
- **unitedstatesclerkofc (“TARGET ACCOUNTS 3”);**

collectively, “**TARGET ACCOUNTS**”), as well as all other subscriber and log records associated with **TARGET ACCOUNTS**, which are located at premises owned, maintained, controlled or operated by TextNow, Inc., an electronic communications service accepting service of process at Attn: Registered Agent of Process for TextNow Inc., GKL Corporate/Search, Inc., Capitol Mall, Suite 660, Sacramento, CA 95814. TextNow Inc. is the United States-based location for TextNow, Inc. of at 420 Wes Graham Way, 2nd Floor, Waterloo, Ontario, Zip Code N2L 0J6, Canada.

ATTACHMENT B**Section I - Information to be disclosed by TextNow, Inc., for search:**

To the extent that the information described in Attachment A is within the possession, custody, or control of **TextNow, Inc.**, regardless of whether such information is located within or outside of the United States, including any messages, records, files, logs, or information that has been deleted but is still available to **TextNow, Inc.**, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f) on March 5, 2021, **TextNow, Inc.** is required to disclose the following information, for the applicable time period specified below, to the government for each account or identifier listed in Attachment A:

- a. Subscriber data associated with **TARGET ACCOUNTS**;
- b. Call logs associated with **TARGET ACCOUNTS**;
- c. Media files associated with **TARGET ACCOUNTS**;
- d. IP address logs associated with **TARGET ACCOUNTS**; and
- e. Message logs, including the content of the messages, associated with **TARGET ACCOUNTS**.
- f. All records pertaining to communications between **TextNow, Inc.** and any person regarding the account, including contacts with support services and records of actions taken.

The applicable time period for the information associated with **TARGET ACCOUNTS** is from account registration date until present.

TextNow, Inc. is hereby ordered to disclose the above information to the government within 14 days of issuance of this warrant.

Section II - Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of Title 18 U.S.C. §§ 912 (Impersonation of an Official of the United States) and 1343, those violations occurring between March 2022 and the present,

1 including, for each account listed on Attachment A, information pertaining to the following
2 matters:

3 a. Any information relating to efforts to impersonate any official of the
4 United States, including but not limited to court personnel and Deputy U.S. Marshals;

5 b. Any information relating to efforts to impersonate any other law
6 enforcement officer;

7 c. Any information regarding efforts to fraudulently obtain funds or to
8 encourage others to send or receive funds from their accounts;

9 d. Any information related to the recipients and senders of monetary
10 instruments;

11 e. Any information regarding opening bank accounts, bank records,
12 checks, credit card bills, account information, and other financial records;

13 f. Any information regarding financial transactions, including the transfer
14 of funds through bank accounts, or the conversion of funds into or from cryptocurrency;

15 g. Any information regarding account logins, including providing access to
16 others through the exchange of login information, or providing verification links;

17 h. Any information that serves to identify any person who uses or access
18 or who exercises in any way any dominion or control over the **TARGET ACCOUNTS**;

19 i. Any information that serves to identify co-conspirators;

20 h. Any content that may identify any alias names, online user names,
21 “handles” and/or “nics” of those who exercise in any way any dominion or control over the
22 accounts as well as records or information that may reveal the true identities of these
23 individuals;

24 j. Any information regarding efforts to evade law enforcement, bank, or
25 regulatory detection;

26 k. Evidence indicating the account owner’s state of mind as it relates to the
27 crimes under investigation;
28

1 l. Any address lists or buddy/contact lists associated with the **TARGET**
2 **ACCOUNTS**;

3 m. All subscriber records associated with the **TARGET ACCOUNTS**,
4 including name, address, local and long distance telephone connection records, or records of
5 session times and durations, length of service (including start date) and types of service
6 utilized, telephone or instrument number or other subscriber number or identity, including
7 any temporarily assigned network address, and means and source of payment for such
8 service) including any credit card or bank account number;

9 n. Any and all other log records, including IP address captures, associated
10 with the specified account; and

11 o. Any records of communications between **TextNow, Inc.**, and any
12 person about issues relating to the account, such as technical problems, billing inquiries, or
13 complaints from other users about the specified account. This to include records of contacts
14 between the subscriber and the provider's support services, as well as records of any actions
15 taken by the provider or subscriber as a result of the communications.

**CERTIFICATE OF AUTHENTICITY OF DOMESTIC
RECORDS PURSUANT TO FEDERAL RULES OF
EVIDENCE 902(11) AND 902(13)**

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by TextNow, Inc., and my title is _____. I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of TextNow, Inc. The attached records consist of _____

[GENERALLY DESCRIBE RECORDS (pages/CDs/megabytes)]. I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of TextNow, Inc., and they were made by TextNow, Inc. as a regular practice; and

b. such records were generated by TextNow, Inc. electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of TextNow, Inc. in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by TextNow, Inc., and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

Date

Signature